What is Claimed is:

1. A method for controlling connectivity in a network comprising:

receiving one or more inputs;

determining a threat level indicator in accordance with said one or more inputs; and

selecting, for use in said network, a firewall configuration in accordance with said threat level indicator.

2. The method of Claim 1, wherein said firewall configuration is selected from a plurality of firewall configurations each associated with a different threat level indicator.

3. The method of Claim 2, wherein a first firewall configuration associated with a first threat level indicator provides for more restrictive connectivity of said network than a second firewall configuration associated with a second threat level indicator when said first threat level indicator is a higher threat level than said second threat level indicator.

4. The method of Claim 3, wherein, a firewall configuration associated with a highest threat level indicator provides for disconnecting said network from all other less-trusted networks.

5. The method of Claim 4, wherein said disconnecting includes physically disconnecting said network from other networks.

6. The method of Claim 4, wherein said network is reconnected to said less trusted networks when a current threat level is a level other than said highest threat level indicator.

7. The method of Claim 1, further comprising:

automatically loading said firewall configuration as a current firewall configuration in use in said network.

8. The method of Claim 1, wherein said one or more inputs includes at least one of: a manual input, a metric about a system in said network, a metric about said network, a derived value determined using a plurality of weighted metrics including one metric about said network, a derived value determined using a plurality of metrics, and an external source from said network.

9. The method of Claim 8, wherein, if said manual input is specified, said manual input determines the threat level indicator overriding all other indicators.

10. The method of Claim 8, wherein said plurality of weighted metrics includes a metric about at least one of: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a high level of privileges.

11. The method of Claim 10, wherein said high level of privileges corresponds to one of: administrator privileges and root user privileges.

12. The method of Claim 1, wherein said selecting additionally selects one or more of the following: an antivirus configuration, an intrusion prevention configuration, and an intrusion detection configuration.

13. A computer program product for controlling connectivity in a network comprising code that:

receives one or more inputs;

determines a threat level indicator in accordance with said one or more inputs; and

selects, for use in said network, a firewall configuration in accordance with said threat level indicator.

14. The computer program product of Claim 13, wherein said firewall configuration is selected from a plurality of firewall configurations each associated with a different threat level indicator.

15. The computer program product of Claim 14, wherein a first firewall configuration associated with a first threat level indicator provides for more restrictive connectivity of said network than a second firewall configuration associated with a second threat level indicator when said first threat level indicator is a higher threat level than said second threat level indicator.

16. The computer program product of Claim 15, wherein, a firewall configuration associated with a highest threat level indicator provides for disconnecting said network from all other less-trusted networks.

17. The computer program product of Claim 16, wherein said code that disconnects includes physically disconnecting said network from other networks.

18. The computer program product of Claim 16, wherein said network is reconnected to said less trusted networks when a current threat level is a level other than said highest threat level indicator.

19. The computer program product of Claim 13, further comprising code that:

automatically loads said firewall configuration as a current firewall configuration in use in said network.

20. The computer program product of Claim 13, wherein said one or more inputs includes at least one of: a manual input, a metric about a system in said network, a metric about said network, a derived value determined using a plurality of weighted metrics including one metric about said network, a derived value determined using a plurality of metrics, and an external source from said network.

21. The computer program product of Claim 20, wherein, if said manual input is specified, said manual input determines the threat level indicator overriding all other indicators.

22. The computer program product of Claim 20, wherein said plurality of weighted metrics includes a metric about at least one of: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a high level of privileges.

23. The computer program product of Claim 22, wherein said high level of privileges corresponds to one of: administrator privileges and root user privileges.

24. The computer program product of Claim 13, wherein said code that selects additionally selects one or more of the following: an antivirus configuration, an intrusion prevention configuration, and an intrusion detection configuration.

25. A method of event reporting by an agent comprising:

receiving data;

determining if said data indicates a first occurrence of an event of interest associated with a metric since a previous periodic reporting;

reporting said first occurrence of an event if said determining determines said data indicates said first occurrence; and

reporting a summary including said metric in a periodic report at a first point in time.

26. The method of Claim 25, wherein said reporting of said first occurrence and said reporting of said summary are performed without a request for a report.

27. The method of Claim 25, wherein data for said reporting of said first occurrence and said reporting of said summary are performed by said agent communicating data at an application level to a reporting destination using a one-way communication connection.

28. The method of Claim 27, wherein said reporting of said first occurrence and said summary further comprising:

opening a communication connection;

sending data to said reporting destination; and

closing said communication connection, said agent only sending data to said reporting destination without reading any communication from said communication connection.

29. The method of Claim 28, wherein said communication connection is a TCP or UDP socket.

30. The method of Claim 25, wherein said periodic report includes a summary of a selected set of one or more data sources and associated values for a time interval since a last periodic report was sent to a reporting destination.

31. The method of Claim 30, wherein said selected set of one or more metrics is a first level of reporting information and said periodic report includes a second level of reporting information used to perform one at least one of the following: determine a cause of a problem, and take a corrective action to a problem.

32. The method of Claim 25, wherein said reporting of said first occurrence and said summary includes transmitting messages from said agent to a reporting destination, each of said messages being a fixed maximum size.

33. The method of Claim 32, wherein a time interval at which said periodic report is sent by said agent and data included in each of said messages are determined in

accordance with at least one of: resources available on a computer system and a network in which said agent is included.

34. The method of Claim 33, wherein said agent executes on a first computer system and reports data to another computer system.

35. The method of Claim 31, further comprising:

monitoring a log file; and

extracting said second level of reporting information from said log file, wherein said log file includes log information about a computer system upon which said agent is executing.

36. The method of Claim 28, wherein said agent transmits an XML communication to said reporting destination using said communication connection.

37. The method of Claim 25, wherein a threshold is specified for an amount of data that said agent can report in a fixed reporting interval, said threshold being equal to or greater than a fixed maximum size for each summary report sent by said agent.

38. The method of Claim 25, wherein a report sent for any of said reporting includes an encrypted checksum preventing modifications of said report while said report is being communicated from an agent to a receiver in a network.

39. The method of Claim 25, wherein said reporting is performed by an agent that sends a report, said report including one of: a timestamp which increases with time duration, and a sequence number which increases with time duration, used by a receiver of said report.

40. The method of Claim 39, wherein said receiver uses said one of said timestamp or said sequence number in authenticating a report received by said receiver as being sent by said agent, said receiver processing received reports having said one of a timestamp or sequence number which is greater than another one of a timestamp or sequence number associated with a last report received from said agent.

41. The method of Claim 31, wherein said second level of reporting information identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

42. A method of event reporting by an agent comprising:

receiving data;

determining if said data corresponds to an event of interest associated with at least one security metric; and

sending a report to a reporting destination, said report including said at least one security metric for a fixed time interval, wherein said report is sent from said agent communicating data at an application level to said reporting destination using a one-way communication connection.

43. The method of Claim 42, wherein said agent only sends data on said one-way communication connection to said reporting destination without reading any communication from said communication connection.

44. The method of Claim 42, wherein said report includes at least one performance metric in accordance with said data received.

45. A method of event reporting by an agent comprising:

receiving data;

determining if said data indicates a security event of interest; and

reporting a summary including information on a plurality of occurrences of said security event of interest occurring within a fixed time interval, said summary being sent at a predetermined time interval.

46. The method of Claim 45, wherein said reporting of said summary is performed without a request for a report.

47. The method of Claim 45, wherein data for said reporting of said summary is performed by said agent communicating data at an application level to a reporting destination using a one-way communication connection.

48. The method of Claim 47, wherein said reporting of said summary further comprises:

opening a communication connection;

sending data to a said reporting destination; and

closing said communication connection, said agent only sending data to said reporting destination without reading any communication from said communication connection.

49. The method of Claim 48, wherein said communication connection is a TCP or UDP socket.

50. The method of Claim 48, wherein said agent transmits an XML communication to said reporting destination using said communication connection.

51. The method of Claim 25, wherein said reporting of said summary includes transmitting periodic messages from said agent to a reporting destination, each of said message having a fixed maximum size.

52. A computer program product for event reporting by an agent comprising code that:

receives data;

determines if said data indicates a first occurrence of an event of interest associated with a metric since a previous periodic reporting;

reports said first occurrence of an event if said code that determines that said data indicates said first occurrence; and

reports a summary including said metric in a periodic report at a first point in time.

53. The computer program product of Claim 52, wherein said code that reports said first occurrence and said code that reports said summary are performed without a request for a report.

54. The computer program product of Claim 52, wherein data for said code that reports said first occurrence and said code that reports said summary are performed by said agent communicating data at an application level to a reporting destination using a one-way communication connection.

55. The computer program product of Claim 54, wherein at least one of said code that reports said first occurrence and said code that reports said summary further comprise code that:

opens a communication connection;

sends data to said reporting destination; and

closes said communication connection, said agent only sending data to said reporting destination without reading any communication from said communication connection.

56. The computer program product of Claim 55, wherein said communication connection is a TCP or UDP socket.

57. The computer program product of Claim 52, wherein said periodic report includes a summary of a selected set of one or more data sources and associated values for a time interval since a last periodic report was sent to a reporting destination.

58. The computer program product of Claim 57, wherein said selected set of one or more metrics is a first level of reporting information and said periodic report includes a second level of reporting information used to perform one at least one of the following: determine a cause of a problem, and take a corrective action to a problem.

59. The computer program product of Claim 52, wherein said code that reports said first occurrence and said code that reports said summary includes code that transmits messages from said agent to a reporting destination, each of said messages being a fixed maximum size.

60. The computer program product of Claim 59, wherein a time interval at which said periodic report is sent by said agent and data included in each of said messages are determined in accordance with at least one of: resources available on a computer system and a network in which said agent is included.

61. The computer program product of Claim 60, wherein said agent executes on a first computer system and reports data to another computer system.

62. The computer program product of Claim 58, further comprising code that:

monitors a log file; and

extracts said second level of reporting information from said log file, wherein said log file includes log information about a computer system upon which said agent is executing.

63. The computer program product of Claim 55, wherein said agent transmits an XML communication to said reporting destination using said communication connection.

64. The computer program product of Claim 52, wherein a threshold is specified for an amount of data that said agent can report in a fixed reporting interval, said threshold being equal to or greater than a fixed maximum size for each summary report sent by said agent.

65. The computer program product of Claim 52, wherein a report sent for any of said code that reports uses an encrypted checksum preventing modifications of said report while said report is being communicated from an agent to a receiver in a network.

66. The computer program product of Claim 52, wherein said code that reports is performed by an agent that sends a report, said report including one of: a timestamp which increases with time duration, and a sequence number which increases with time duration, used by a receiver of said report.

67. The computer program product of Claim 66, wherein said receiver uses said one of said timestamp or said sequence number in authenticating a report received by said receiver as being sent by said agent, said receiver processing received reports having said one of a timestamp or sequence number which is greater than another one of a timestamp or sequence number associated with a last report received from said agent.

68. The computer program product of Claim 58, wherein said second level of reporting information identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

69. A computer program product for event reporting by an agent comprising code that:

receives data;

determines if said data corresponds to an event of interest associated with at least one security metric; and

sends a report to a reporting destination, said report including said at least one security metric for a fixed time interval, wherein said report is sent from said agent communicating data at an application level to said reporting destination using a one-way communication connection.

70. The computer program product of Claim 69, wherein said agent only sends data on said one-way communication connection to said reporting destination without reading any communication from said communication connection.

71. The computer program product of Claim 69, wherein said report includes at least one performance metric in accordance with said data received.

72. A computer program product for event reporting by an agent comprising code that:

receives data;

determines if said data indicates a security event of interest; and

reports a summary including information on a plurality of occurrences of said security event of interest occurring within a fixed time interval, said summary being sent at a predetermined time interval.

73. The computer program product of Claim 72, wherein said code that reports said summary is performed without a request for a report.

74. The computer program product of Claim 72, wherein data for said code that reports said summary is performed by said agent communicating data at an application level to a reporting destination using a one-way communication connection.

75. The computer program product of Claim 74, wherein said code that reports said summary further comprises code that:

opens a communication connection;

sends data to a said reporting destination; and

closes said communication connection, said agent only sending data to said reporting destination without reading any communication from said communication connection.

76. The computer program product of Claim 75, wherein said communication connection is a TCP or UDP socket.

77. The computer program product of Claim 75, wherein said agent transmits an XML communication to said reporting destination using said communication connection.

78. The computer program product of Claim 52, wherein said code that reports said summary includes code that transmits periodic messages from said agent to a reporting destination, each of said message having a fixed maximum size.

79. A method of event notification comprising:

receiving a first report of a condition;

sending a first notification message about said first report of said condition;

sending a second notification message about said condition at a first notification interval;

receiving subsequent reports at fixed time intervals;

sending a subsequent notification message at a second notification interval if said condition is still ongoing during said second notification interval, wherein said second notification interval has a length which is a multiple of said first notification interval.

80. The method of Claim 79, wherein said first report is sent from a reporting agent on a first computer system reporting about one of: said first computer system and a network including said first computer system, and said notification messages are sent from a notification server on a second computer system.

81. The method of Claim 79, wherein notification messages are sent to a notification point at successive notification intervals wherein each of said successive notification intervals increases approximately exponentially with respect to an immediately prior notification interval.

82. The method of Claim 80, wherein said condition is associated with an alarm condition and an alarm condition is set when a current level of a metric is not in accordance with a predetermined threshold value.

83. The method of Claim 79, wherein each of said notification messages includes a first level of information about said condition and a second level of information used to perform at least one of the following: determine a cause of said condition, and take a corrective action for said condition.

84. The method of Claim 83, wherein an option is included in a reporting agent to enable and disable reporting of said second level of information to a notification server from said agent sending said first report.

85. The method of Claim 83, wherein an option is used to enable and disable condition notification messages including said second level of information.

86. The method of Claim 82, wherein an alarm condition is associated with a first level alarm and an alarm state of said first level is maintained when a current level of a metric is in accordance with said predetermined threshold value until an acknowledgement of said alarm state at said first level is received by said notification server.

87. The method of Claim 86, wherein said alarm condition transitions to a second level alarm when said current level is not in accordance with said predetermined threshold and another threshold associated with a second level, and said second level alarm is maintained when a current level of a metric is in accordance with one of: said

predetermined threshold and said other threshold until acknowledgement of said second level alarm is received by said notification server.

88. The method of Claim 79, wherein reports are sent from a reporting agent executing on a computer system in an industrial network to an appliance included in said industrial network and each of said reports includes events occurring within said industrial network.

89. The method of Claim 82, wherein an alarm condition is determined in accordance with a plurality of weighted metrics, said plurality of weighted metrics including at least one metric about: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a level of privileges greater than a level associated with a user-level account.

90. A method of event notification comprising:

receiving a first report of a condition at a reporting destination; and

sending a notification message from said reporting destination to a notification destination, said notification message including a summary of information about events occurring in a fixed time interval, said summary identifying at least one of: a source and a target associated with an attack occurring within said fixed time interval, and a percentage of events associated with said at least one of said source and said target.

91. The method of Claim 90, wherein said summary identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

92. The method of Claim 90, wherein said summary identifies at least one target associated with an attack, wherein said target is one of: a user, a machine, an application, and a port, said percentage indicating a percentage of events associated with said at least one target for a type of attack.

93. The method of Claim 90, wherein said summary identifies a portion of a type of attack represents with respect to all attacks in said fixed time interval.

94. A method of event notification comprising:

receiving report of a potential cyber-attack condition at fixed time intervals; and

sending a notification message about said conditions when said conditions exceed a notification threshold.

95. The method of Claim 94, wherein a notification threshold is determined using an alarm condition in accordance with a plurality of weighted metrics, said plurality of weighted metrics including at least one metric about: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a level of privileges greater than a level associated with a user-level account.

96. The method of Claim 94, wherein said notification message includes a summary of information about events occurring in a fixed time interval, said summary identifying at least one of: a source and a target associated with an attack occurring within said fixed time interval, and a percentage of events associated with said at least one of said source and said target.

97. The method of Claim 96, wherein said summary identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

98. The method of Claim 96, wherein said summary identifies at least one target associated with an attack, wherein said target is one of: a user, a machine, an application, and a port, said percentage indicating a percentage of events associated with said at least one target for a type of attack.

5

99. The method of Claim 96, wherein said summary identifies a portion of a type of attack represents with respect to all attacks in said fixed time interval.

100. A computer program product for event notification comprising code that:

receives a first report of a condition;

sends a first notification message about said first report of said condition;

sends a second notification message about said condition at a first notification interval;

receives subsequent reports at fixed time intervals; and

sends a subsequent notification message at a second notification interval if said condition is still ongoing during said second notification interval, wherein said second notification interval has a length which is a multiple of said first notification interval.

101. The computer program product of Claim 100, wherein said first report is sent from a reporting agent on a first computer system reporting about one of: said first computer system and a network including said first computer system, and said notification messages are sent from a notification server on a second computer system.

102. The computer program product of Claim 100, wherein notification messages are sent to a notification point at successive notification intervals wherein each of said successive notification intervals increases approximately exponentially with respect to an immediately prior notification interval.

103. The computer program product of Claim 101, wherein said condition is associated with an alarm condition and an alarm condition is set when a current level of a metric is not in accordance with a predetermined threshold value.

104. The computer program product of Claim 100, wherein each of said notification messages includes a first level of information about said condition and a second level of information used to perform at least one of the following: determine a cause of said condition, and take a corrective action for said condition.

105. The computer program product of Claim 104, wherein an option is included in a reporting agent to enable and disable reporting of said second level of information to a notification server from said agent sending said first report.

106. The computer program product of Claim 104, wherein an option is used to enable and disable condition notification messages including said second level of information.

107. The computer program product of Claim 103, wherein an alarm condition is associated with a first level alarm and an alarm state of said first level is maintained when a current level of a metric is in accordance with said predetermined threshold value until an acknowledgement of said alarm state at said first level is received by said notification server.

108. The computer program product of Claim 107, wherein said alarm condition transitions to a second level alarm when said current level is not in accordance with said predetermined threshold and another threshold associated with a second level, and said

second level alarm is maintained when a current level of a metric is in accordance with one of: said predetermined threshold and said other threshold until acknowledgement of said second level alarm is received by said notification server.

109. The computer program product of Claim 100, wherein reports are sent from a reporting agent executing on a computer system in an industrial network to an appliance included in said industrial network and each of said reports includes events occurring within said industrial network.

110. The computer program product of Claim 103, wherein an alarm condition is determined in accordance with a plurality of weighted metrics, said plurality of weighted metrics including at least one metric about: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a level of privileges greater than a level associated with a user-level account.

111. A computer program product for event notification comprising code that:

receives a first report of a condition at a reporting destination; and

sends a notification message from said reporting destination to a notification destination, said notification message including a summary of information about events occurring in a fixed time interval, said summary identifying at least one of: a source and a target associated with an attack occurring within said fixed time interval, and a percentage of events associated with said at least one of said source and said target.

112. The computer program product of Claim 111, wherein said summary identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

113. The computer program product of Claim 111, wherein said summary identifies at least one target associated with an attack, wherein said target is one of: a user, a machine, an application, and a port, said percentage indicating a percentage of events associated with said at least one target for a type of attack.

114. The computer program product of Claim 111, wherein said summary identifies a portion of a type of attack represents with respect to all attacks in said fixed time interval.

115. A computer program product for event notification comprising code that:

receives report of a potential cyber-attack condition at fixed time intervals; and

sends a notification message about said conditions when said conditions exceed a notification threshold.

116. The computer program product of Claim 115, wherein a notification threshold is determined using an alarm condition in accordance with a plurality of weighted metrics, said plurality of weighted metrics including at least one metric about: a network intrusion detection, a network intrusion prevention, a number of failed login attempts, a number of users with a level of privileges greater than a level associated with a user-level account.

117. The computer program product of Claim 115, wherein said notification message includes a summary of information about events occurring in a fixed time interval, said summary identifying at least one of: a source and a target associated with an attack occurring within said fixed time interval, and a percentage of events associated with said at least one of said source and said target.

118. The computer program product of Claim 117, wherein said summary identifies at least one source associated with an attack, wherein said source is one of: a user, a machine, and an application, said percentage indicating a percentage of events associated with said at least one source for a type of attack.

119. The computer program product of Claim 117, wherein said summary identifies at least one target associated with an attack, wherein said target is one of: a user, a machine, an application, and a port, said percentage indicating a percentage of events associated with said at least one target for a type of attack.

5

120. The computer program product of Claim 117, wherein said summary identifies a portion of a type of attack represents with respect to all attacks in said fixed time interval.

121. A method for monitoring an industrial network comprising:

reporting first data about a first computer system by a first agent executing on said first computer system in said industrial network, said first computer system performing at least one of: monitoring or controlling a physical process of said industrial network, said first data including information about software used in connection with said physical process.

122. The method of Claim 121, further comprising:

reporting second data about communications on a connection between said industrial network and another network by a second agent executing on a second computer system.

123. The method of Claim 122, wherein said second data reported by said second agent is included in an appliance to which said first data is sent.

124. The method of Claim 121, wherein said first agent reports on at least one of: critical file monitoring, log file for said first computer system, hardware and operating system of said first computer system, password and login, a specific application executing on said computer system wherein said application is in accordance with a particular industrial application of said industrial network.

125. The method of Claim 124, wherein a plurality of agents execute on said first computer system monitoring said first computer system.

126. The method of Claim 125, wherein said plurality of agents includes a master agent and other agents performing a predetermined set of monitoring tasks, said master agent controlling execution of said other agents.

127. The method of Claim 126, wherein said plurality of agents report data at predetermined intervals to one of: an appliance and said second computer system.

128. The method of Claim 127, further comprising performing, by at least one of said plurality of agents:

obtaining data from a data source;

parsing said data;

performing pattern matching on said parsed data to determine events of interest;

recording any events of interest;

reporting any events of interest in accordance with occurrences of selected events in a time interval;

creating a message including said summary at predetermined time intervals; and

encrypting at least one of: said message and a checksum of said message.

129. The method of Claim 121, wherein said first data includes at least one of the following metrics: a number of open listen connections and a number of abnormal process terminations.

130. The method of Claim 129, wherein, when a number of open listen connections falls below a first level, an event corresponding to a component failure is determined.

131. The method of Claim 129, wherein, when a number of open listen connections is above a second level, an event corresponding to a new component or unauthorized component is determined.

132. The method of Claim 122, wherein said second agent reports on network activity in accordance with a set of rules, said rules including at least one rule indicating that events in a business network are flagged as suspicious in said industrial network.

133. The method of Claim 132, wherein said events include at least one of: an event associated with a web browser, and an event associated with e-mail.

134. The method of Claim 122, wherein said second agent reports on an address binding of a physical device identifier to a network address if the physical device identifier of a component was not previously known, or said network address in the address binding is a reassignment of said network address within a predetermined time period since said network address was last included in an address binding.

135. The method of Claim 122, wherein said second agent reports second data about a firewall, and said second data includes at least one of: a change to a saved

firewall configuration corresponding to a predetermined threat level, a change to a current set of firewall configuration rules currently controlling operations between said industrial network and said other network.

136. The method of Claim 135, wherein log files associated with said firewall are stored remotely at a location on said second computer system with log files for said second computer system activity.

137. The method of Claim 122, wherein said second data includes at least one threat assessment from a source external to said industrial network.

138. The method of Claim 137, wherein said second data includes at least one of: a threat level indicator from a corporate network connected to said industrial network, a threat level indicator from a public network source, and a threat level indicator that is manually input.

139. The method of Claim 121, further comprising:

receiving at least said first data by a receiver;

authenticating said first data as being sent by said first agent; and

processing, in response to said authenticating, said first data by said receiver.

140. The method of Claim 139, wherein said authenticating includes at least one of: verifying use of said first agent's encryption key, and checking validity of a message checksum, and using a timestamp or sequence number to detect invalid reports received by said receiver as being sent from said first agent.

141. The method of Claim 121, wherein said reporting is performed in accordance with a threshold size indicates an amount of data that said first agent is permitted to transmit in a fixed periodic reporting interval.

142. A computer program product for monitoring an industrial network comprising code that:

reports first data about a first computer system by a first agent executing on said first computer system in said industrial network, said first computer system performing at least one of: monitoring or controlling a physical process of said industrial network, said first data including information about software used in connection with said physical process.

143. The computer program product of Claim 142, further comprising code that:

reports second data about communications on a connection between said industrial network and another network by a second agent executing on a second computer system.

144. The computer program product of Claim 143, wherein said second data reported by said second agent is included in an appliance to which said first data is sent.

145. The computer program product of Claim 142, wherein said first agent reports on at least one of: critical file monitoring, log file for said first computer system, hardware and operating system of said first computer system, password and login, a specific application executing on said computer system wherein said application is in accordance with a particular industrial application of said industrial network.

146. The computer program product of Claim 145, wherein a plurality of agents execute on said first computer system monitoring said first computer system.

147. The computer program product of Claim 146, wherein said plurality of agents includes a master agent and other agents performing a predetermined set of monitoring tasks, said master agent controlling execution of said other agents.

148. The computer program product of Claim 147, wherein said plurality of agents report data at predetermined intervals to one of: an appliance and said second computer system.

149. The computer program product of Claim 148, further comprising code for performing, by at least one of said plurality of agents:

obtaining data from a data source;

parsing said data;

performing pattern matching on said parsed data to determine events of interest;

recording any events of interest;

reporting any events of interest in accordance with occurrences of selected events in a time interval;

creating a message including said summary at predetermined time intervals; and

encrypting at least one of: said message and a checksum of said message.

150. The computer program product of Claim 142, wherein said first data includes at least one of the following metrics: a number of open listen connections and a number of abnormal process terminations.

151. The computer program product of Claim 150, wherein, when a number of open listen connections falls below a first level, an event corresponding to a component failure is determined.

152. The computer program product of Claim 150, wherein, when a number of open listen connections is above a second level, an event corresponding to a new component or unauthorized component is determined.

153. The computer program product of Claim 143, wherein said second agent reports on network activity in accordance with a set of rules, said rules including at least one rule indicating that events in a business network are flagged as suspicious in said industrial network.

154. The computer program product of Claim 153, wherein said events include at least one of: an event associated with a web browser, and an event associated with e-mail.

155. The computer program product of Claim 143, wherein said second agent reports on an address binding of a physical device identifier to a network address if the physical device identifier of a component was not previously known, or said network

address in the address binding is a reassignment of said network address within a predetermined time period since said network address was last included in an address binding.

156. The computer program product of Claim 143, wherein said second agent reports second data about a firewall, and said second data includes at least one of: a change to a saved firewall configuration corresponding to a predetermined threat level, a change to a current set of firewall configuration rules currently controlling operations between said industrial network and said other network.

157. The computer program product of Claim 156, wherein log files associated with said firewall are stored remotely at a location on said second computer system with log files for said second computer system activity.

158. The computer program product of Claim 143, wherein said second data includes at least one threat assessment from a source external to said industrial network.

159. The computer program product of Claim 158, wherein said second data includes at least one of: a threat level indicator from a corporate network connected to said industrial network, a threat level indicator from a public network source, and a threat level indicator that is manually input.

160. The computer program product of Claim 142, further comprising code that:

receives at least said first data by a receiver;

authenticates said first data as being sent by said first agent; and

processes, in response to said code that authenticates, said first data by said receiver.

161. The computer program product of Claim 160, wherein said code that authenticates includes at least one of: code that verifies use of said first agent's encryption key and checks validity of a message checksum, and code that uses a timestamp or sequence number to detect invalid reports received by said receiver as being sent from said first agent.

162. The computer program product of Claim 142, wherein said code that reports uses a threshold size indicating an amount of data that said first agent is permitted to transmit in a fixed periodic reporting interval.

163. A method for detecting undesirable messages in a network comprising:

receiving a message in said network;

determining if said message is undesirable in accordance with at least one rule defining an acceptable message in said network; and

reporting said message as undesirable if said message is not determined to be in accordance with said at least one rule.

164. The method of Claim 163, further comprising:

defining another rule for use in said determining if an additional message type is determined to be acceptable in said network.

165. A computer program product for detecting undesirable messages in a network comprising code that:

receives a message in said network;

determines if said message is undesirable in accordance with at least one rule defining an acceptable message in said network; and

reports said message as undesirable if said message is not determined to be in accordance with said at least one rule.

166. The computer program product of Claim 165, further comprising code that:

defines another rule for use in said determining if an additional message type is determined to be acceptable in said network.

167. A method for performing periodic filesystem integrity checks comprising:

receiving two or more sets of filesystem entries, each set representing a grouping of one or more filesystem entries;

selecting zero or more entries from each set; and

performing integrity checking for each selected entry from each set during a reporting period.

168. The method of Claim 167, wherein each of said two or more sets correspond to a predetermined classification level.

169. The method of Claim 168, wherein if a first classification level is more important than a second classification level, said first classification level includes less entries than said second classification level.

170. The method of Claim 168, wherein a number of entries from each set is determined in accordance with a level of importance associated with said set.

171. A computer program product for performing periodic filesystem integrity checks comprising code that:

receives two or more sets of filesystem entries, each set representing a grouping of one or more filesystem entries;

selects zero or more entries from each set; and

performs integrity checking for each selected entry from each set during a reporting period.

172. The computer program product of Claim 171, wherein each of said two or more sets correspond to a predetermined classification level.

173. The computer program product of Claim 172, wherein if a first classification level is more important than a second classification level, said first classification level includes less entries than said second classification level.

174. The computer program product of Claim 172, wherein a number of entries from each set is determined in accordance with a level of importance associated with said set.